Conduct of Business Affairs

EC 38015892

January, 1998

Index

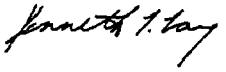
Foreword

As officers and employees of Enron Corp., its subsidiaries, and its affiliated companies, we are responsible for conducting the business affairs of the companies in accordance with all applicable laws and in a moral and honest manner.

To be sure that we understand what is expected of us, Enron has adopted certain policies, with the approval of the Board of Directors, which are set forth in this booklet. I ask that you read them carefully and completely and that, as you do, you reflect on your past actions to make certain that you have complied with the policies. It is absolutely essential that you fully comply with these policies in the future. If you have any questions, talk them over with your supervisor, manager, or Enron legal counsel.

We want to be proud of Enron and to know that it enjoys a reputation for fairness and honesty and that it is respected. Gaining such respect is one aim of our advertising and public relations activities, but no matter how effective they may be, Enron's reputation finally depends on its people, on you and me. Let's keep that reputation high.

January 30, 1998



Kenneth L. Lay
Chairman and Chief
Executive Officer

How to Use this Booklet

Enron has long had a set of written policies dealing with rules of conduct to be used in conducting the business affairs of Enron Corp., its subsidiaries, and its affiliated companies (collectively the "Company"). It is very important that you understand the scope of those policies and learn the details of every one that relates to your job.

In order to do this, please take the following steps:

1. Carefully read the summaries of each of the Enron policies in this booklet;
2. If you have a concern or question, talk it over with your supervisor, manager, or Enron legal counsel; and/or
3. Report your concerns or possible violations to the Enron Corp. Compliance Officer as described in the section on Responsibility for Reporting at page 51 of this booklet.

Enclosed with this booklet is a Certificate of Compliance to be signed by you as a statement of your personal agreement to comply with the policies stated herein during the term of your employment with the Company. Please carefully review this booklet, then sign and return the Certificate of Compliance to Elaine V. Overturf, Deputy Corporate Secretary and Director of Stockholder Relations, Enron Corp.

These policies are not an employment contract. Enron does not create any contractual rights by issuing these policies.

The Company reserves the right to amend, alter, and terminate policies at any time.

Securities Trades By Company Personnel

No director, officer, or employee of Enron Corp. or its subsidiaries or its affiliated companies (collectively referred to herein as "Company") shall, directly or indirectly, trade in the securities of Enron Corp., Enron Oil & Gas Company, Northern Border Partners, L.P., EOTT Energy Partners, L.P., or any other Enron Corp. subsidiary or affiliated company with publicly-traded securities, or any other publicly-held company while in the possession of material non-public information relating to or affecting any such companies, disclose such information to others who may trade, or recommend the purchase or sale of securities of a company to which such information relates. Advice should be sought in respect of equivalent requirements under other applicable jurisdictions.

The Need For A Policy Statement

The Securities and Exchange Commission ("SEC") and the Justice Department actively pursue violations of insider trading laws. Historically, their efforts were concentrated on individuals directly involved in trading abuses. In 1988, to further deter insider trading violations, Congress several years ago expanded the authority of the SEC and the Justice Department, adopting the Insider Trading and Securities Fraud Enforcement Act (the "Act"). In addition to increasing the penalties for insider trading, the Act puts the onus on companies and possibly other "controlling persons" for violations by company personnel.

Although the Act is aimed primarily at the securities industry, application of the laws may be made to companies in other industries. Many experts have concluded that if companies like Enron Corp. do not take active steps to adopt preventive policies and procedures covering securities trades by company personnel, the consequences could be severe.

In addition to responding to the Act, we are adopting this Policy Statement to avoid even the appearance of improper conduct on the part of anyone employed by or associated with the Company (not just so-called insiders). We have all worked hard over the years to establish our reputation for integrity and ethical conduct. We cannot afford to have it damaged.

The Consequences

This policy applies to all employees of the Company. It is intended to provide guidance to employees with respect to existing legal restrictions. It is not intended to result in the imposition of liability on employees that would not exist in the absence of such policy. Any breach of this policy, however, may subject employees to criminal penalties.

The consequences of insider trading violations can be staggering:

For individuals who trade on inside information (or tip information to others):

- A civil penalty of up to three times the profit gained or loss avoided;
- A criminal fine (no matter how small the profit) of up to $1 million; and
- A jail term of up to ten years.

For a company (as well as possibly any supervisory person) that fails to take appropriate steps to prevent illegal trading:

- A civil penalty of the greater of $1 million or three times the profit gained or loss avoided as a result of the employee's violation; and
- A criminal penalty of up to $2.5 million.

Moreover, if an employee violates the Company insider trading policy, the Company imposed sanctions, including dismissal for cause, could result.

Our Policy

If a director, officer, or any employee of the Company (as defined herein) has material non-public information relating to Enron Corp., Enron Oil & Gas Company, Northern Border Partners, L.P., EOTT Energy Partners, L.P., or any other Enron Corp. subsidiary or affiliated company with publicly-traded securities, it is the Company's policy that neither that person nor any related person may buy or sell securities of Enron Corp., Enron Oil & Gas Company, Northern Border Partners, L.P., EOTT Energy Partners, L.P., or other Enron Corp. subsidiary or affiliated company with publicly traded securities, or engage in any other action to take advantage of, or pass on to others, that information. This policy also applies to material non-public information relating to any other company, including our customers or suppliers, obtained in the course of employment.

Transactions that may be necessary or justifiable for independent reasons (such as the need to raise money for an emergency expenditure) are no exception. Even the appearance of an improper transaction must be avoided to preserve the Company's reputation for adhering to the highest standards of conduct.

Material Information. Material information is any information that a reasonable investor would consider important in a decision to buy, hold, or sell stock: in short, any information which could reasonably be expected to affect the price of the stock. If you are considering buying or selling a security because of information you possess, you should assume such information is material.

Examples. Common examples of information that will frequently be regarded as material are: projections of future earnings or losses; news of a pending or proposed merger, acquisition, or tender offer; news of a significant sale of assets or the disposition of a subsidiary; changes in dividend policies or the declaration of a stock split or the offering of additional securities; changes in management; significant new products or discoveries; impending bankruptcy or financial liquidity problems; and the gain or loss of a substantial customer or supplier. Either positive or negative information may be material. The foregoing list is by no means exclusive.

Twenty-Twenty Hindsight. If your securities transactions become the subject of scrutiny, they will be viewed after-the-fact with the benefit of hindsight. As a result, before engaging in any transaction you should carefully consider how regulators and others might view your transaction in hindsight.

Transactions By Family Members. The very same restrictions apply to your family members and others living in your household. Employees are expected to be responsible for the compliance of their immediate family and personal household.

Tipping Information To Others. Whether the information is proprietary information about the Company or information that could have an impact on our stock prices, employees must not pass material non-public information on to others; this is called tipping. The above penalties may apply, whether or not you derive any direct benefit from another's actions.

When Information Is Public. Information is "non-public" until it has been disseminated in a manner making it available to investors generally. This is typically satisfied by distribution of such information by means of a press release. However, even after such information is released to the press, you should wait a period of time (at least one business day and often two or three business days) before trading or disclosing such information to others. Again, it is a good idea to exercise caution and wait a longer period of time following the release of material information than you might first consider warranted.

Company Assistance

No set of specific rules will be adequate in every circumstance. Any person who has any questions about specific transactions may obtain additional guidance from Elaine Overturf, Deputy Corporate Secretary and Director of Stockholder Relations, at (713) 853-6062, who will consult with Company counsel as appropriate. Remember, however, the ultimate responsibility for adhering to the Policy Statement and avoiding improper transactions rests with you. In this regard, it is imperative that you act in good faith and use your best judgment.

EC 38015896.1

Employees of Enron Corp., its subsidiaries, and its affiliated companies (collectively the "Company") are charged with conducting their business affairs in accordance with the highest ethical standards. An employee shall not conduct himself or herself in a manner which directly or indirectly would be detrimental to the best interests of the Company or in a manner which would bring to the employee financial gain separately derived as a direct consequence of his or her employment with the Company. Moral as well as legal obligations will be fulfilled openly, promptly, and in a manner which will reflect pride on the Company's name.

Products and services of the Company will be of the highest quality and as represented. Advertising and promotion will be truthful, not exaggerated or misleading.

Agreements, whether contractual or verbal, will be honored. No bribes, bonuses, kickbacks, lavish entertainment, or gifts will be given or received in exchange for special position, price, or privilege.

Employees will maintain the confidentiality of the Company's sensitive or proprietary information and will not use such information for their personal benefit.

Relations with the Company's many publics – customers, stockholders, governments, employees, suppliers, press, and bankers – will be conducted in honesty, candor, and fairness.

Employees will comply with the executive stock ownership requirements set forth by the Board of Directors of Enron Corp., if applicable.

Laws and regulations affecting the Company will be obeyed. Even though the laws and business practices of foreign nations may differ from those in effect in the United States, the applicability of both foreign and U.S. laws to the Company's operations will be strictly observed. Illegal behavior on the part of any employee in the performance of Company duties will neither be condoned nor tolerated.

Trade Secrets and Confidential Information

You may have access to or become aware of confidential and/or proprietary information of the Company - that is, information relating to the Company's business which is not generally or publicly known. This information includes but is not limited to:

> Internal telephone lists and directories; bid, trading, and financial data; planned new projects and ventures; advertising and marketing programs; lists of potential or actual customers and suppliers; wage and salary or other personnel data; capital investment plans; changes in management or policies of the company; suppliers' prices; and other trade secrets.

The term "trade secret" means any type of information that has independent economic value because it is not generally known or publicly ascertainable by proper means and the owner has taken reasonable measures to keep it confidential.

The Company's confidential or proprietary information could be very helpful to suppliers and the Company's competitors, to the detriment of the Company. To help protect the Company's interests, business units have established and implemented computer and electronic security measures to ensure that employees have the means to communicate domestically and internationally in a secure fashion. Employees should follow these guidelines:

- No employee may use, either for his/her own personal benefit or for the benefit of others, Company information that is not publicly known;
- No employee should disclose trade secrets or proprietary or confidential information to other employees or outsiders, except as required in the conduct of the Company's business;

- Dispose of documents containing the Company's confidential or proprietary information with care so as to avoid inadvertent disclosure; and
- Guard against inadvertently disclosing such information in public discussions where you may be overheard and in discussions with family members or friends.

Information about Others

Our employees have a duty and legal obligation to respect the confidentiality rights of others. In the normal course of doing business, it is common to acquire information about other companies and current or potential customers, suppliers, or competitors. You should respect the proprietary nature of this information and not use it or reveal it to others.

In 1996, the U.S. Congress passed the Economic Espionage Act which provides significant criminal penalties for persons who engage in the theft of trade secrets.

In addition, the Economic Espionage Act prohibits you from acquiring confidential or proprietary information (including technology) about other companies through improper means, such as deceit, misrepresentation, or receipt of information illegally acquired by a third party, or from present or former employees who are not authorized to disclose it.

Safety

Employees of the Company have a responsibility to comply with all applicable laws and regulations regarding the safe design, construction, maintenance, and operation of Company facilities. It is the responsibility of every employee to perform his or her work and conduct the Company's operations in a safe manner. Employees should be aware that health and safety laws may provide for significant civil and criminal penalties against individuals and/or the Company for failure to comply with applicable requirements. Accordingly, each employee must comply with all applicable safety and health laws, rules, and regulations, including occupational safety and health standards.

All information, ideas, concepts, improvements, discoveries, and employee inventions, whether patentable or not, which are conceived, made, developed, or acquired by an employee, individually or in conjunction with others, during the employee's employment by Enron Corp., its subsidiaries, and its affiliated companies (collectively the "Company") (whether during business hours or otherwise and whether on the Company's premises or otherwise) which relate to the Company's business, products, or services shall be disclosed to the Company and are and shall be the sole and exclusive property of the Company.

For this purpose, the Company's business, products, or services, include, without limitation, all such information relating to corporate opportunities, research, financial and sales data, pricing and trading terms, evaluations, opinions, interpretations, acquisition prospects, the identity of customers or their requirements, the identity of key contacts within the customer's organizations (or within the organization of acquisition prospects), or marketing and merchandising techniques, and prospective names and marks.

Moreover, all documents, drawings, memoranda, notes, records, files, correspondence, drawings, manuals, models, specifications, computer programs, E-mail, voice mail, electronic databases, maps, and all other writings or materials of any type embodying any of such information, ideas, concepts, improvements, discoveries, and inventions are and shall be the sole and exclusive property of the Company.

If, during employee's employment by the Company, employee creates any original work of authorship fixed in any tangible medium of expression which is the subject matter of copyright (such as videotapes, written presentations on acquisitions, computer programs, E-mail, voice mail, electronic databases, drawings, maps, architectural renditions, models, manuals, brochures, or the like) relating to the Company's business, products, or services, whether such work is created solely by employee or jointly with others (whether during business hours or otherwise and whether on Company's premises or otherwise), employee shall disclose such work to Company.

The Company shall be deemed the author of such work if the work is prepared by employee in the scope of his or her employment; or, if the work is not prepared by employee within the scope of his or her employment but is specially ordered by the Company as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, or as an instructional text, then the work shall be considered to be work made for hire and the Company shall be the author of the work. If such work is neither prepared by the employee within the scope of his or her employment nor a work specially ordered and is deemed to be a work made for hire, then employee hereby agrees to assign, and by these presents does assign, to the Company all of employee's worldwide right, title, and interest in and to such work and all rights of copyright therein.

As a result of employee's employment by the Company, employee may also from time to time have access to, or knowledge of, confidential business information or trade secrets of third parties, such as customers, suppliers, partners, joint venturers, and the like, of the Company. Each employee also agrees to preserve and protect the confidentiality of such third party confidential information and trade secrets to the same extent, and on the same basis, as the Company's confidential business information and trade secrets.

These obligations of confidence apply irrespective of whether the information has been reduced to a tangible medium of expression (e.g., is only maintained in the minds of Company's employees) and, if it has been reduced to a tangible medium, irrespective of the form or medium in which the information is embodied (e.g., documents, drawings, memoranda, notes, records, files, correspondence, manuals, models specifications, computer programs, E-mail, voice mail, electronic databases, maps, and all other writings or materials of any type.)

Each employee agrees to act with honesty, candor, and fairness with respect to competitors and third parties and to comply in all respects with applicable laws prohibiting the misappropriation of trade secrets, copyright infringement, or use of counterfeit or spurious trademarks. Under no circumstances will any activity be authorized or undertaken

by an employee which violates the federal Economic Espionage Act, the federal Copyright Act, the federal Trademark Counterfeiting Act, or any other applicable domestic or foreign laws.

More specifically, all employees must recognize that the term "trade secret" means any type of information that has independent economic value because it is not generally known or publicly ascertainable by proper means and which the third party owns and has taken reasonable measures to keep confidential.

An employee will not knowingly:

(1) take, carry away, or obtain a third party secret without authorization or obtain a third party trade secret by fraud or deception;

(2) copy, download, mail, deliver, send, transmit, or communicate a third party trade secret without authorization; or

(3) receive, buy, or possess a third party trade secret knowing it has been stolen or obtained without authorization.

Further, if an employee uses trade secrets of a former employer without the former employer's permission, this conduct violates the federal Economic Espionage Act. An employee will not willfully infringe for purposes of commercial advantage or private financial gain a third party's copyright in a work by copying the work, distributing copies of the work, using the work to prepare derivative works, or in the case of some works, to publicly display or perform the work.

An employee will not intentionally traffic in goods or services using a counterfeit or spurious trademark. All employees should be aware that a violation of applicable domestic or foreign laws, particularly the federal Economic Espionage Act, the federal Copyright Act, or the federal Trademark Counterfeiting Act, may result in the imposition of significant civil and criminal penalties for the Company as well as for the individual employees.

The federal Economic Espionage Act, which also applies to conduct that benefits any foreign government, foreign instrumentality, or foreign

agent, provides for criminal fines for the Company of up to $10 Million and criminal fines for an employee of up to $500,000 and up to 15 years imprisonment. The federal Copyright Act provides for criminal fines for an employee of up to $250,000 and up to 5 years imprisonment for the first offense. The federal Trademark Counterfeiting Act provides for criminal fines for the Company of up to $1 Million and criminal fines for an employee of up to $250,000 and up to 5 years imprisonment for the first offense.

If an employee has any questions concerning the meaning of the laws, the employee should contact the Company's General Counsel.

Upon signing the Certificate of Compliance, an employee acknowledges and agrees that:

1. the business of the Company is highly competitive, and its strategies, methods, books, records, and documents, its technical information concerning its products, equipment, services, and processes, procurement procedures and pricing techniques, and the names of and other information (such as credit and financial data) concerning its customers and its business affiliates all comprise confidential business information and trade secrets which are valuable, special, and unique assets which the Company uses in its business to obtain a competitive advantage over its competitors;

2. the protection of such confidential business information and trade secrets against unauthorized disclosure and use is of critical importance to the Company in maintaining its competitive position;

3. he or she will not, at any time during or after his or her employment by the Company, make any unauthorized disclosure of any confidential business information or trade secrets of the Company, or make any use thereof, except in the carrying out of his or her employment responsibilities hereunder;

4. the Company shall be a third party beneficiary of the employee's obligations under this policy; and

5. he or she agrees to act with honesty, candor, and fairness with respect to competitors and third parties, and to comply in all respects with applicable laws prohibiting the misappropriation of trade secrets, copyright infringement, or the use of counterfeit or spurious trademarks.

All documents, drawings, memoranda, notes, records, files, correspondence, manuals, models, specifications, computer programs, E-mail, voice mail, electronic databases, maps, and all other writings or materials of any type made by, or coming into possession of, employee during the period of employee's employment by the Company which contain or disclose confidential business information or trade secrets of the Company shall be and remain the property of the Company. Upon termination of employee's employment by the Company, for any reason, employee promptly shall deliver the same, and all copies thereof, to the Company.

Policy on Use of Communication Services and Equipment

The term "Communication Services and Equipment" as used in this Policy and the accompanying Procedures shall mean any and all communications systems or equipment owned or possessed by Enron Corp., its divisions, subsidiaries, and its affiliated and related companies (the "Company"), or used in connection with the Company's business, including but not limited to, telephones, facsimile machines, computers, computer modems, special long-distance services, cellular phones, voice mail, pagers, electronic mail, mail and delivery services, storage means of all types for the physical or electronic storage of the Company's information or data, transaction services, or any other services of any nature whatsoever in connection with any communication systems necessary or desirable to promote the conduct of the Company's business.

General application of this Policy and the accompanying Procedures

This Policy and the accompanying Procedures apply to all employees, third party contractors, guests, licensees, or invitees of the Company who utilize, possess, or have access to the Company's Communication Services and Equipment (cumulatively referred to herein as the "Users" of the Company's Communication Services and Equipment).

General Policy of the Company with respect to its Communication Services and Equipment

It is the general policy of Company:

- To provide or contract for effective Communication Services and Equipment for use by the Company in connection with its business;
- To preserve and protect the confidentiality of the information and data of the Company and its customers and contractors;

- To preserve and protect the legal privileges provided by the law with respect to attorney/client communications, work product, and investigations of the Company and its customers and contractors; and
- To operate and maintain the Company's Communication Services and Equipment in a manner that is in full compliance with the law.

Limits on expectations of privacy

All Users of the Company's Communication Services and Equipment are advised and placed on notice that:

1. The United States government, and the various State and local governments, may monitor contemporaneous communications of all types (including communication by telephone, facsimile machine, computer modems, special long-distance services, cellular phones, voice mail, pagers, electronic mail, mail, and other delivery services) or access stored communications, data, or information of all types, subject to the protections of the Fourth Amendment of the United States Constitution, which generally requires the issuance of a court order or warrant. Moreover, the United States government, and the various State and local governments, may monitor contemporaneous oral, wire, or electronic communications of all types subject to federal statutes such as First Amendment Privacy Protection Act and the Omnibus Crime Control and Safe Streets Act as amended by the Electronic Communications Privacy Act of 1986.
2. The Federal Rules of Civil Procedure and the rules of civil procedure for almost all States permit requests for production of documents that are likely to lead to the discovery of relevant evidence. Both the Federal Rules of Civil Procedure and the Texas Rules of Civil Procedure specifically allow the discovery of electronically maintained data. For example, Rule 34 of the Federal Rules of Civil Procedure and Rule 166b(2)(b) of the Texas Rules of Civil

Procedure permit the discovery of data compilations from which information can be obtained, translated, if necessary, by the respondent through detective devices into reasonably readable form.

3. There should be no expectations of privacy whatsoever with respect to communications sent to or received from public electronic bulletin boards or public electronic communications systems such as the Internet.

4. Under the regulations of the United States Postal Service, any mail addressed to a non-governmental organization, including but not limited to corporations, firms, sole proprietorships, partnerships, joint ventures and associations, or an individual, such as an official, employee, contractor, client, agent, etc. by name or title at the address of the organization, shall be delivered to the organization. This is also true with respect to mail addressed in this manner to former officials, employees, contractors, agents, clients, etc. Moreover, mail addressed in this manner but bearing the term "personal" is no different from other mail and shall be delivered by the United States Postal Service to the Company. For example, the United States Postal Service will deliver each of the following to the offices of the Company:

Sam Smith Enron Corp. 1400 Smith Street P.O. Box 1188 Houston, Texas 77251	Sam Smith 1400 Smith Houston, Texas 77251	Sam Smith Personal and Confidential P.O. Box 1188 Houston, Texas 77251

All such mail belongs to the Company until such time as the Company determines that the information contained in the mail does not pertain to the business of the Company. The Company shall have the right to open the mail if there is some question as to its deliverability and/or forward the mail to a superior or Company designated recipient if the person to whom the mail is addressed is no longer with the Company or is ill or on extended leave.

EC 38015902.1

Moreover, all incoming or outgoing mail containing information owned by the Company is the property of the Company and the Company has the right to open any Company mail in order to protect its business interests or to prevent illegal conduct.

5. The Company reserves the right to openly and on a continuous basis monitor the contemporaneous communications of certain of its functions, such as the monitoring of the telephones used in connection with certain training functions and the telephones on the floors in which certain of its traders operate. There should be no expectation of privacy by anyone with respect to communications conducted on those telephones.

6. The Company reserves the right to monitor on a contemporaneous basis communications transmitted by or stored within its Communication Services and Equipment in the ordinary course of the Company's business to ensure that no improper, illegal, or criminal activities or being conducted. Such monitoring shall be effected in accordance with the provisions of the Omnibus Crime Control and Safe Streets Act as amended by the Electronic Communications Privacy Act of 1986 and only if authorized by an officer of the Company.

7. The Company reserves the right to delete or destroy any and all communications, including E-mail and voice mail messages, stored in the Company's Communication Services and Equipment. As a general rule, the Company's Communication Services and Equipment is not backed-up and should, therefore, be thought of as a very temporary storage media. If a machine failure in the Company's Communication Services and Equipment occurs, all messages and data could be lost. Therefore, Users must not consider E-mail and voice mail messages to be permanently stored by the Company. On the other hand, the Company also reserves the right in its discretion to maintain any and all communications, including E-mail and voice mail messages, transmitted by or stored within the Company's Communication Services and Equipment. Users therefore also should take care that the messages they transmit or store comply with all of the Company's policies and with the law.

8. The Company reserves the right to access E-mail messages, voice mail messages, data, or information stored on the Company's computers or other electronic devices or media owned or controlled by the Company or comprising the Company's Communication Services and Equipment. Therefore, there should be no expectation of privacy with respect to such stored E-mail messages, voice mail messages, data, or information.

9. Because all of the Company's Communication Services and Equipment are the property of the Company, the Company reserves the right to monitor its Communication Services and Equipment in order to ensure that its property is being properly and legally used.

10. Users do not have a personal privacy right in any data or information created, received, or sent on the Company's Communication Services and Equipment. Any data or information transmitted or stored on the Company's Communication Services and Equipment, whether or not they relate or pertain to the Company's business, goods, or services, may be accessed by the Company. Any employee or contractor who elects to utilize the Company's Communication Services and Equipment to transmit or store data or information recognizes that the Company may access and monitor such data or information and has no obligation to continue to store such data and information.

Ownership and confidentiality of information

1. All of the Company's Communication Services and Equipment are the property of the Company. Any and all communication, data, or information created, received, or sent on the Company's Communication Services and Equipment are the property of Company. Users have no right, title, or interest in such Communication Services and Equipment or in any communications,

data, or information created, received, or sent on the Company's Communication Services and Equipment. All means of identifying communications, such as the use of domain names on the Internet or other networks or systems, that embody or use the Company's image, names, or marks (such as an Internet domain name incorporating Enron.Com) shall belong to the Company.

2. This *Policy* and the accompanying *Procedures* do not modify in any way the Company's policy that the Company is and remains the owner of all information created by the Company's employees during their employment by the Company that relates to the business, goods, or services of the Company, irrespective of where such information is stored or maintained, e.g., in electronic form on the hard drives of the Company's computers, in electronic form in servers maintained by the Company as part of its network, or in diskettes or computers purchased by the Company that are possessed by the employees.

3. This *Policy* and the accompanying *Procedures* do not modify in any way the Company's policy that Users remain obligated to protect the confidentiality of the Company's information irrespective of where such information is stored or maintained, e.g., in electronic form on the hard drives of the Company's computers, in electronic form in servers maintained by the Company as part of its network, or in diskettes or computers purchased by the Company that are possessed by the employees.

The right to use the Company's Communication Services and Equipment is at the will of the Company and is conditioned on continued compliance with the Company's rules and policies

1. Users are allowed to utilize the Company's Communication Services and Equipment only at the will and discretion of the Company. The Company has the right to prohibit Users from utilizing the Company's Communication Services and Equipment at any time for any reason.

2 Moreover, the Users' right to use the Company's Communication Services and Equipment is conditioned on acceptance of the terms of this ***Policy*** and the accompanying ***Procedures*** as well as continued compliance with this and all of the Company's other rules and policies.

Acceptance, disciplinary action, interpretation, and modification

Employment by the Company, agreement by a contractor to do business with the Company, or use of the Company's Communication Services and Equipment by a User, constitutes acceptance of and consent to the terms of this ***Policy*** and the accompanying ***Procedures***.

Improper use of the Company's Communication Services and Equipment may result in discipline, up to and including termination.

Questions about interpretation of this ***Policy*** and the accompanying ***Procedures*** should be referred to the Company's Human Resources Department, the Law Department or the Information Services Department.

Procedures for Use of Communications Services and Equipment

Purpose

To set forth the procedures for the use of the Company's Communication Services and Equipment in accordance with the Policy.

General application of this Policy and the accompanying Procedures

This ***Policy*** and the accompanying ***Procedures*** apply to all Users of the Company's Communication Services and Equipment.

Requirements for the use of the Company's Communication Services and Equipment

1. The Company's Communication Services and Equipment should be used for Company purposes only. Employees should limit use of the Company Communication Services and Equipment for personal purposes to those circumstances where such personal use enhances such employee's efficiency during office hours or otherwise does not detract from such employee's activities on behalf of the Company. When personal usage is unavoidable, employees must properly log any user charges and reimburse the Company for them. However, whenever possible, personal communications that incur user charges should be placed on a collect basis or charged directly to the employee's personal credit card or account. Users may not use the Company's Communication Services and Equipment for non-Company businesses, such as "moonlighting" jobs.

2. Users should not utilize the Company's communications systems to send or receive private, personal messages they do not wish monitored or accessed by the government, third parties, or the Company.

3. Users shall refrain absolutely from any activity that may cause harm or damage to the Company's Communication Services and Equipment or any communications, data, or information transmitted by or stored within such Communication Services and Equipment.

4. Users may not use the Company's Communication Services and Equipment for or in connection with any illegal or criminal activity. Users may not use the Company's Communication Services and Equipment for any activity which violates any Company policy. For example, Users may not use the Company's Communication Services and Equipment to copy, duplicate, or use software that is not properly licensed or the use of which infringes the copyright of a third party. Users may not use the Company's Communication Services and Equipment to infringe third party intellectual property rights. Accordingly, Users should download information and software from the Internet and other public or third party systems into communications systems and equipment only when such downloads do not infringe on third party copyrights or intellectual property rights.

5. No confidential or proprietary information of the Company and no privileged communications (e.g., attorney/client communications) may be transmitted via public electronic communication systems unless the transmissions are properly encrypted and no third party copyright or intellectual property rights are violated.

6. Users may not use the Company's Communication Services and Equipment to forward messages without a legitimate business purpose under circumstances likely to lead .o embarrassment of the sender or to violate a clearly expressed desire of the sender to restrict additional dissemination.

7. Users may not connect incompatible equipment to the Company's Communication Services and Equipment. Users may not use in the Company's Communication Services and Equipment any software that is infected with a virus. If any such software is found to be infected with a virus, users will immediately alert those who have received a copy, and work with their systems management to remove the virus.

8. All employees and contractors must recognize and always keep in mind that whatever they reduce to a tangible form and maintain in their physical or electronic files may possibly, under the

appropriate circumstances, be discovered by third parties in litigation. Employees and contractors are cautioned that all such documents must comply with the Company's policies with respect to the protection of confidential information, the Company's policies with respect to the protection of privileged communications, and the Company's document retention policies.

9. Users may not use the Company's Communication Services and Equipment for "chain" letters.

10. Users should keep the number of messages and data stored in the Company's Communication Services and Equipment under control, and purge old Communication Services and Equipment messages and data regularly.

11. Employees should exercise care so that no personal correspondence appears to be an official communication of the Company. Personalized Company stationery and business cards may only be issued by the Company and may only be used in connection with Company business. Employees may not use the Company's address for receiving personal mail or use Company stationery or postage for personal matters.

PASSWORDS

Users should change their passwords at least quarterly, every 90 days Passwords should be no shorter than six characters and should be a mixture of alpha, special, and numeric symbols so that the password code is difficult for others to determine using "password cracking" software.

Passwords should not contain any codes, names, words, or phrases that someone familiar with the owner might associate with that person and thereby have an advantage in cracking the code and using it illegally.

Passwords are not to be shared by two or more people. Each User should have a unique code that only they know.

Files containing User account names, log on codes, and passwords (i.e. security files) in Company Communication Services and Equipment should be examined at least weekly for persons who no longer work for the Company, and their access authority immediately removed.

Users who have not used their access identification code and password for longer than 90 consecutive calendar days should have their need for continued access reviewed at least monthly.

All Company Communication Services and Equipment that allow persons to connect to the service or equipment from a remote location (dial-up access) should require all Users to authenticate themselves through the use of passwords or other types of technology, such as voice recognition systems, that ensure the person is who they say they are

Whenever possible, all remote access Company Communication Services and Equipment should have a preset maximum number of attempts to authenticate the remote User, e.g. 3 attempts. Failure to successfully remotely authenticate within three attempts should result in that access session being terminated, or forwarded to a Company security officer for verification of the requesting party.

MONITORING COMMUNICATION SERVICES AND EQUIPMENT ACCESS

All Company Communication Services and Equipment should be designed/equipped to accurately and quickly determine and log all attempted or successful intrusions of the system or network by someone not authorized to use that system or network. Any such "hacker" attempts should be immediately investigated and measures taken quickly to prevent that type of unauthorized access in the future.

INTERNET SECURITY POLICY: SCOPE OF USE OF ELECTRONIC MEDIA AND SERVICES

Introduction - General Application Of This Policy

This Internet Security Policy defines roles, responsibilities, and policies for the Company's employees, agents, and contractors using the Company's communications facilities to access third party electronic media and services such as the Internet.

As an advanced technology company, we increasingly use and exploit electronic forms of communication and information exchange. Company employees, agents, and contractors may have access to one or more forms of electronic media and services, computers, e-mail, telephones, voicemail, fax machines, external electronic bulletin boards, wire services, on-line services, and the Internet.

The Company encourages the use of these media and associated services because information technology is part of our business, because they make communication more efficient and effective, and because they are valuable sources of information about vendors, customers, new products, and services. However, Company-provided access to electronic media and services (e.g. an Internet account) are the Company's property, and their purpose is to facilitate Company business.

With the rapidly changing nature of electronic media, and the "netiquette" which is developing among users of external on-line services and the Internet, this Internet Policy cannot lay down rules to cover every possible situation. Instead, this Internet Policy expresses the Company's philosophy and sets forth general principles to be applied to use of electronic media and services. This Internet Policy applies to all Company employees, agents, and contractors using electronic media and services which are: accessed on or from Company premises; accessed using Company computer equipment, or via Company-paid access methods; and/or used in a manner which identifies the individual with the Company collectively, and individually, such individuals will be referred to as "Internet Users".

Use of Company-provided access to the Internet is intended to be primarily for the Company's business-related purposes. Internet access is monitored, and actual web-site connections are recorded. Excessive use of Company-provided access to the Internet for non-business-related purposes will result in loss of access privileges.

Procedures, Guidelines, And Restrictions

Accounts and Account Passwords

(a) You are responsible for the security of your account password(s) and will be held responsible for all use or misuse of your account. You must maintain secure passwords to your account. Internet Users accessing the Internet over a Company network may be required to use an ID and password at the firewall (in addition to their usual LAN sign on). Passwords are machine generated and will be changed every thirty days. You must follow all directions of the Company's system administrators with respect to security of passwords and take reasonable precautions against unauthorized access.

(b) Remote login to the Company network is prohibited unless permission to do so is granted. Do not remotely log into (or otherwise use) any workstation or computer not designated explicitly for public logins over the Company network— even if the configuration of the computer permits remote access — unless you have explicit permission from the owner and the current user of that computer to log into that machine.

(c) Access to selected Internet hosts or networks which the Company designates as inappropriate may be denied. You may not use any account set up for another user and you may not attempt to find out the password of a service for which you have not been authorized, including accounts set up for other users.

(i) File Transfer Protocol "FTP" may be used to initiate transfer of data from/to specified Company hosts and from/to selected Internet hosts. Initiation of FTP sessions to Company hosts from the Internet is prohibited.

(ii) Access to "network news" is allowed with restrictions. The Company will apply filters as appropriate to block certain news groups.

(iii) Access to the "World Wide Web" is permitted. Inappropriate sites may be blocked from the Company network.

(iv) All services not explicitly allowed are prohibited. Use of games or other non-work related objects over the Internet is prohibited.

(d) Network services and World Wide Web sites can and do monitor access and usage and can identify at least which company — and often which specific individual — is accessing their services. Thus, accessing a particular bulletin board or Website leaves Company-identifiable electronic "tracks" even if the Internet User merely reviews or downloads the material and does not post any message. As a general rule, all Internet use should be conducted with this in mind so as to always portray the Company as a reputable company and to maintain its reputation and goodwill.

Intended Uses

Electronic media and services are primarily for Company business use. All Company systems and related equipment are intended for the communication, transmission, processing, and storage of Company-authorized information. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable — as is the case with personal phone calls. However, Internet Users need to demonstrate a sense of responsibility and may not abuse the privilege.

(a) Electronic media may not be used for knowingly transmitting, retrieving, or storing any communication which is (i) discriminatory, harassing, or threatening (ii) derogatory to any individual, (iii) obscene , (iv) defamatory or threatening , (v) a "chain letter" or junk mail, (vi) untrue or fraudulent, or (vi) illegal or against Company policy or contrary to the Company's interest, or for personal profit.

(b) In downloading any material from the World Wide Web or by FTP transfer, or in distributing any material by e-mail or FTP transfer, you must bear in mind any proprietary or intellectual property rights of third parties in the material. You must not and may not copy material where such copying would infringe the proprietary or intellectual property rights of third parties. Such infringement is an offense which may render you liable for civil claims and, where appropriate, may also be a criminal offense.

(c) You may not download or store any material from the World Wide Web, or received by e-mail or by FTP transfer, or distribute any material by FTP transfer or by e-mail, which is indecent or obscene.

(d) No e-mail or other electronic communications may be sent which attempt to hide the identify of the sender, or represent the sender as someone else or from another company. Whenever Users send e-mail, User name, User ID, and the Company's name are included in each e-mail message. Internet Users are solely responsible for all electronic mail originating from their user id. When using the Company's e-mail facilities, the following are prohibited: (i) forgery or attempted forgery of e-mail messages; and (ii) reading, deleting, copying, or modifying the e-mail of others.

(e) Employees must respect the confidentiality of other people's electronic communications and may not attempt to (i) "hack" into third party systems, (ii) read other people's logins or "crack" passwords, (iii) breach computer or network security measures,

EC 38015908.1

or (iv) intercept or monitor electronic files or communications of other employees or third parties, except by explicit direction of Company management.

(f) Many software programs and computer data, and related materials such as documentation, are owned by individual users or other companies, and are protected by copyright and other laws, together with licenses and other contractual arrangements. Anyone obtaining electronic access to another company's or individual's materials must respect all rights (including copyrights) therein, and may not copy, retrieve, modify, disclose, examine, rename, or forward such materials except as permitted by the person owning the data, software programs, and/or other materials. Such restrictions include:

(i) copying programs or data;

(ii) reselling programs or data;

(iii) using programs or data for non-Company business purposes;

(iv) using programs or data for personal financial gain;

(v) using programs or data without being one of the licensed individuals or groups; and

(vi) publicly disclosing information about software programs without the owner's permission.

FAILURE TO ABIDE BY THESE RESTRICTIONS MAY SUBJECT EMPLOYEES TO CIVIL AND/OR CRIMINAL PROSECUTION.

Consent to Monitoring

Electronic information created and/or communicated by an Internet User using e-mail, word processing, utility programs, spreadsheets, voicemail, telephones, Internet/Bulletin Board System (BBS) access, etc. may be monitored by the Company and the Company reserves the right to monitor especially with respect to the following:

(a) The Company routinely monitors usage patterns for both voice and data communications (e.g., number called or site accessed; call length; times of day when calls were initiated). Reasons include cost analysis/allocation and the management of our gateway to the Internet.

(b) The Company also reserves the right, in its discretion, and the employee upon signing the Certificate of Compliance consents to such action from the Company to review and disclose any electronic files and messages (including e-mail) and usage to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other Company policies. The Company may also find it necessary to monitor the system for signs of illegal or unauthorized entry. Accordingly, the Company reserves the right, in its discretion, and the undersigned hereby consents to such action by the Company, to intercept and disclose any electronic files and messages (including e-mail) at any time with or without prior notification to the users or owners of such files or resources. The undersigned hereby waives any right to privacy in such electronic files.

(c) Employees should therefore understand that electronic communications are not totally private and confidential. Sensitive or confidential information should be transmitted by more secure means.

Assuring Proper Use of The Company's System Resources

Electronic media and services should be used in an efficient and economical manner and not in a way that is likely to cause network congestion or significantly hamper the ability of other people to access and use the Company's computer systems. Any software that is designed to destroy data, provide unauthorized access to the Company's computer systems, or disrupt computing processes is prohibited.

Confidentiality and Encryption

In accordance with the Policy on Use of Communication Services and Equipment, Internet Users will maintain the confidentiality of the Company's confidential and/or proprietary information and will not use such information for their personal benefit. Any messages or information sent by an Internet User to one or more individuals via an electronic network (e.g., bulletin board, on-line service, or Internet) are statements identifiable and attributable to the Company. While some users include personal "disclaimers" in electronic messages, it should be noted that there would still be a connection with the Company, and the statement might still be legally imputed to the Company. All communications sent by employees via a network must comply with this and other Company policies and may not disclose any confidential and/or proprietary Company information.

To ensure the Company's continuous access to information on the Company's computer systems, no Internet User shall use personal hardware or software to encrypt any e-mail, voicemail, or any other data stored in or communicated by the Company's computer systems, except in accordance with express prior written permission from the Company's management. Should an Internet User have a need to use security measures to encrypt any e-mail, voicemail, or any other data stored in or communicated by the Company's computer systems, such user should contact the appropriate information systems personnel to assist in and facilitate such encryption. The Company will retain the encryption keys for all encrypted data stored in or communicated by the Company's

computer systems, except in accordance with express prior written permission from the Company's management. There may be a need for the Company to access an Internet User's system or files when he/she is away from the office, therefore, Company management, at their discretion, may request that authorized systems personnel reset the password of an Internet User who uses any security measures on an Company-supplied PC, Macintosh, UNIX workstation, or any other Company-supplied workstation for Company use if required.

To meet the Company's public disclosure responsibilities as required by the Securities and Exchange Commission and to ensure that we are communicating a consistent message, public disclosure restrictions apply to interactions over the Internet as well as any other methods of communications. Any employee found to be abusing the privilege of Company-facilitated access to electronic media or services will be subject to corrective action up to and including termination, risk losing Internet User privileges, and/or having the privilege removed for himself/herself and possibly other employees.

Any unauthorized attempts to penetrate or subvert Company computer systems will be thoroughly and promptly investigated and resolved on a case-by-case basis. If circumstances warrant, such attempts will be vigorously pursued and prosecuted to the full extent of the law.

EC 38015910.1

Governmental Affairs and Political Contributions

The Company's official policy concerning all governmental, political, and public matters in which the Company has an interest will be determined and announced by the Executive Committee of Enron Corp.'s Board of Directors. No alteration of or deviation from such official policy will be made without the approval of the Chairman of the Board and Chief Executive Officer of Enron Corp.

The Company employs governmental relations and public policy personnel who are assigned the responsibility of fulfilling its corporate public affairs responsibility, communicating with public bodies and officials pertaining to the Company's position on public policy questions, and maintaining the goodwill and understanding of public officials.

Communications of the Company's position to public officials or bodies by personnel of the Company and its subsidiaries must be coordinated with the governmental relations and public policy personnel at corporate headquarters.

The Company may also provide factual information to employees and stockholders concerning the impact on the Company of specific issues, legislation, and other governmental, political, and public matters. Such communications must be approved by the Chairman of the Board and Chief Executive Officer of Enron Corp. or the President and Chief Operating Officer of Enron Corp.

To establish restrictions with regard to corporate participation in the political system as imposed by law, the following guidelines will be followed:

1. No funds, assets, or services of the Company will be used for political contributions, directly or indirectly, unless allowed by applicable foreign and U.S. law and approved in advance by the Chairman of the Board or President of Enron Corp.

2. Company contributions to support or oppose public referenda or similar ballot issues are permitted, with advance approval of the Chairman of the Board or President of Enron Corp.

3. Employees, if eligible under applicable foreign and U.S. law, may make political contributions through legally established Company sponsored and approved political support funds. Any such personal contribution is not a deductible expense for federal or other applicable income tax purposes and is not eligible for reimbursement by the Company as a business expense. Political action committees are permitted under U.S. law.

Under no circumstances will any activity be authorized or undertaken by an employee which violates the provisions of the Foreign Corrupt Practices Act, federal and state election laws, bribery, or other applicable domestic or foreign laws.

The Company encourages its employees, management, and stockholders to exercise their voting rights and take an active interest and participate in public affairs at local, state, and national levels.

Employees, regardless of their Company position, are free to express their views on public affairs matters through political or non-political measures of their choice and engage in partisan political activities. Employees should conduct themselves in contacts with others so as to make clear that the views expressed are their own and not those of the Company.

olimible under applicable foreign and U.S. law, may

Consulting Fees, Commissions, and Other Payments

Agreements with consultants, agents, or representatives must be in writing and must state the services to be performed, the fee basis, amounts to be paid, and other material terms and conditions, and the form and content must be approved by the Company's legal counsel and with respect to foreign consultants, agents, or representatives by the Company's Vice Chairman, Mr. Jack Urquhart. Payments must bear a reasonable relationship to the value of the services rendered, must be completely documented and recorded, and must not violate the provisions of the Foreign Corrupt Practices Act or any other applicable law, including, without limitation, those relating to bribery. Payments will be made by check or wire transfer in accordance with the following procedure:

1. In any lawful currency in the country where the services are performed; and

2. To the person directly or to the person's bank account in the country where the services are performed; provided, however, that payment may be made other than in the place of performance with the approval of Company legal counsel.

When payments are requested to be made in any manner, currency, or place other than in accordance with the above procedure, the person who has made such request shall be advised that such payments shall not be made except upon notification to the governments of both the country of residence and the country where the services are performed, unless Company legal counsel determines that such notice is not required by law and is not otherwise advisable under the circumstances. Such notification shall be made to both governments even though the requested manner of payment does not apparently violate applicable domestic or foreign law. Notification with respect to the requested manner of payment should normally be made to the tax, finance, or other governmental authorities, as shall be appropriate under the circumstances.

The Company policy discourages but does not prohibit customary expediting payments to low-level employees of foreign governments, properly recorded in the Company's books, which are not excessive in amount and which meet the following criteria:

1. The making of such payments is an established and well-recognized practice in the area.

2. Such payments are to expedite or assure performance of a routine governmental action (such as obtaining customs clearances, visas, and work permits) to which the Company or the Company's employee is clearly entitled.

3. The payment does not violate any provisions of the Foreign Corrupt Practices Act or any applicable law, including, without limitation, those relating to bribery.

prohibit customary expe-

Compliance with the Foreign Corrupt Practices Act

The United States Foreign Corrupt Practices Act (the "Act") applies to the Company in its worldwide operations as well as individually to all Company employees who are United States citizens, nationals, or residents with respect to their worldwide activities. The Act prohibits the corrupt offer, payment or gift of money or anything of value to a foreign governmental official or employee or to any foreign political candidate or party for the purpose of influencing any act or decision of a governmental body in order to obtain or retain business or to direct business to any person. The Act also prohibits the offer, payment or gift of money or anything of value to any third party with knowledge that all or a portion of such money or thing of value will be transferred to a governmental official or employee or political candidate for the prohibited purposes. The Act contains certain narrow affirmative defenses to its prohibitions.

The Act provides for criminal and civil penalties. Criminal sanctions of up to $2,000,000 per offense can be imposed on the Company and fines of up to $100,000 per offense and imprisonment for up to 5 years can be imposed on individuals convicted of violating the Act. Company policy requires strict compliance with the Act.

Due to the broad nature of the Act's prohibitions, it may be implicated by a wide range of activities in addition to direct bribery of a foreign official. For instance, arrangements with foreign joint venture partners, foreign agency or sponsorship arrangements, and any direct dealings with, including lavish entertainment of, foreign governmental officials or employees may raise issues under the Act.

Any questions with respect to the application of the Act to any proposed activity by the Company should be referred immediately to Company legal counsel.

Compliance with Antitrust Laws

All employees of the Company are expected to comply fully with all applicable federal, state, and foreign antitrust laws. Whenever any doubt exists as to the legality of any action or arrangement, such transaction must be submitted to Company legal counsel for prior approval and continuing review. Both the spirit and the letter of antitrust laws are to be followed, so as to avoid creating any unlawful restraints on competition or the appearance of any unlawful restraints.

In the United States, certain types of agreements with third party persons, including competitors, suppliers, or customers, are unlawful per se under federal antitrust law. That is to say, such agreements are automatically in violation of such laws, regardless of the agreement's commercial reasonableness, its purpose, or actual effect on competition. Other agreements with competitors or customers, although not unlawful per se, may be unlawful under the antitrust "rule of reason."

Formal or informal arrangements with actual or potential competitors (a broadly defined group) which limit or restrict competition may constitute per se violations. Such unlawful agreements include those which: fix, stabilize, or control prices (also a broadly defined term which includes not only price but any element of price such as credit terms, discounts, freight rates etc.) or terms or conditions of sale; allocate products, markets, customers, or territories; boycott customers or suppliers; or limit or prohibit a party form carrying on a particular commercial enterprise. To assure compliance with antitrust laws, Company employees are not to enter into any discussion or arrangement with an actual or potential competitor which could result in any such per se violation. Further, since the existence of an unlawful agreement may be inferred from the mere exchange of competitively sensitive information between competitors, absent prior review and approval by Company counsel that such actions are lawful no employee shall give to or accept from a competitor any information concerning prices, terms, and conditions of sale, or any other competitive information.

Certain types of restrictive understandings between a customer and supplier are also deemed to be anticompetitive and may be per se antitrust violations. Some such agreements are clearly per se illegal, such as an agreement between a supplier and a distributor setting the distributor's minimum resale prices. Others may be per se illegal if the party imposing the agreement has market power, such as an agreement imposing a requirement of reciprocal dealing, (for example, an agreement that one party buys goods from another only on the understanding that the second party will buy goods from the first), or tying a customer's right to buy one product or service to the obligation to buy another. These possible per se illegal arrangements must not be agreed to or discussed with a customer, absent prior review and approval by Company counsel that the arrangement is lawful.

Agreements that do not unambiguously injure competition (i.e., that are not per se illegal) are analyzed under the antitrust rule of reason. Under the antitrust "rule of reason" test, a court determines whether a particular agreement acts as an "unreasonable" restraint on trade and thus is anticompetitive and unlawful. Such a determination is based on a particular set of facts and circumstances, including the terms of the agreement, the purposes, the relationship of the parties, and the probable effects on competition. Since the circumstances surrounding any arrangement change from time to time, it is essential that agreements which could potentially cause an unreasonable restraint on trade be subject to continuing review by Company legal counsel.

Unilateral action by the Company (in other words, conduct not involving an agreement) may also violate the antitrust laws. Any transaction or practice that would appear to result in the Company gaining a monopoly in a particular line of business in a particular market or geographic area, or which indicates an intent to drive a competitor out of business or to prevent a competitor from entering a market, should therefore be avoided and discussed with Company legal counsel.

Also, discriminating pricing can violate a complicated antitrust statute known as the Robinson-Patman Act.

The sanctions resulting from violations of the antitrust laws can be severe, both as to corporations and as to individuals; they include both criminal penalties and civil treble damages. Whenever any question arises as to the significance or application of antitrust laws, Company legal counsel must be consulted, and any agreements with possible antitrust implications shall be made only with prior approval of Company legal counsel.

International operations may be subject to antitrust laws of either the United States or foreign countries, so employees should be aware of the implication of any such laws to Company transactions.

Advice should be sought in respect of equivalent requirements under other applicable jurisdictions, including the European Commission.

Compliance with Environmental Laws

Employees of Enron Corp., its subsidiaries, and its affiliated companies (collectively the "Company") must conduct Company operations in compliance with all applicable environmental laws and regulations including those of other countries which have jurisdiction over Company activities. These laws are designed to protect the environment in which we live and work, human health, wildlife, and natural resources. Environmental laws either prohibit or severely restrict the release of pollutants to the air, land, surface water, and groundwater. They contain numerous waste management requirements. They impose on owners and operators of most types of facilities the duty to protect the environment by requiring them to obtain permits for certain emissions, to report releases and spills of materials which may cause pollution, and to create and maintain certain records. The Company is committed to environmental protection, and it expects employees to abide by the letter and the spirit of these laws. Employees who do not follow environmental rules and regulations shall be subject to appropriate disciplinary action.

Those responsible for the construction and the operation of Company facilities must ensure that the Company has the necessary environmental permits and clearances for these activities and that the Company complies with the terms and conditions of its permits. These individuals are charged with the responsibility of ensuring that the Company makes all required environmental reports and maintains, at the appropriate location, all required environmental records. Employees must consider the environmental consequences of all aspects of Company operations and proposed changes to our operations.

One of the major environmental laws of the United States may have significant legal and economic consequences for companies which fail to consider the environmental aspects of proposed transactions. The Comprehensive Environmental Response, Compensation and Liability Act (CERCLA, commonly known as "Superfund") was passed to provide a means for cleaning up abandoned waste disposal sites and for

responding to environmental emergencies. CERCLA imposes sweeping liability (i) on those who sent hazardous substances to sites that may be cleaned up under CERCLA, (ii) on those who owned or operated these sites when hazardous substances were sent there, (iii) on those who transported hazardous substances to these sites, and (iv) on those who now own or operate these sites. These four classes of persons are potentially responsible for the entire cost of cleaning up the site. Employees must attempt to avoid actions which would increase the Company's Superfund liability. Those who are responsible for disposing waste offsite should ensure that the disposal facility is well managed by a reputable firm. Those who engage in real estate transactions of any nature, particularly acquiring property rights, should make all appropriate inquiry about environmental conditions at the property before completing the real estate transaction.

Environmental regulations change constantly both in the United States and abroad. Those who are responsible for environmental compliance should make every effort to stay abreast of changes to regulations which affect the Company and to plan accordingly for the implementation of regulations which have been proposed.

Environmental audits may be used to verify compliance with environmental regulations. The U.S. Environmental Protection Agency and the Department of Justice encourage the performance of periodic, internal environmental audits to ensure compliance with regulatory requirements. The Company likewise encourages those in charge of operations to conduct periodic environmental audits of Company facilities.

The Company encourages the efforts of employees to minimize the quantity of waste generated by Company operations and to recycle waste which is produced. Innovative waste minimization not only protects the environment by reducing the volume of waste generated, it may also result in reduced operating costs for the Company.

All employees should be aware that the violation of environmental laws may result in the imposition of significant civil and criminal penalties for the Company as well as for individual employees. Many of the laws that apply to the Company's operations in the U.S. provide for civil penalties

in the amount of $25,000 per violation, and they make each day of violation a separate offense. Criminal penalties for environmental violations may be as much as fifteen (15) years imprisonment per violation. Severe criminal and civil penalties for environmental violations may also be imposed in other countries in which the Company conducts its business.

Advice should be sought with respect to requirements and powers of enforcement agencies in jurisdictions outside of the United States.

Investments and Outside Business Interests of Officers and Employees

Employees of the Company have inquired from time to time as to the propriety of their association with, or the investment of their personal funds in, business enterprises similar in character to certain activities of the Company. In response, the Company has established certain principles for the guidance of officers and employees with respect to personal business and investment interests.

The primary consideration of the employment of every full-time (regular as well as temporary) officer and employee should be the fact that the employer is entitled to expect of every such person complete loyalty to the best interests of the Company and the maximum application of skill, talent, education, etc., to the discharge of job responsibilities, without any reservations whatever. Therefore, it follows that no full-time officer or employee should:

(a) Engage in any outside activity or enterprise which could interfere in any way with job performance,

(b) Make investments or perform services for his or her own or related interest in any enterprise under any circumstances where, by reason of the nature of the business conducted by such enterprise, there is, or could be, a disparity or conflict of interest between the officer or employee and the Company; or

(c) Own an interest in or participate, directly or indirectly, in the profits of any other entity which does business with or is a competitor of the Company, unless such ownership or participation has been previously disclosed in writing to the Chairman of the Board and Chief Executive Officer of Enron Corp. and such officer has determined that such interest or participation does not adversely affect the best interests of the Company.

Notwithstanding any provision to the contrary in this Policy on Investments, securities of publicly owned corporations which are regularly traded on the open market may be owned without disclosure if they are not purchased as a result of confidential knowledge about

the Company's operations, relations, business, or negotiations with such corporations.

If an investment of personal funds by an officer or employee in a venture or enterprise will not entail personal services or managerial attention, and if there appears to be no conflict or disparity of interest involved, the following procedure nevertheless shall be followed if all or any part of the business of the venture or enterprise is identical with, or similar or directly related to, that conducted by the Company, or if such business consists of the furnishing of goods or services of a type utilized to a material extent by the Company:

(a) The officer or employee desiring to make such investment shall submit in writing to the Chairman of the Board and Chief Executive Officer of Enron Corp. a brief summary of relevant facts; and

(b) The Chairman of the Board and Chief Executive Officer of Enron Corp. shall consider carefully the summary of relevant facts, and if he concludes that there appears to be no probability of any conflict of interest arising out of the proposed investment, the officer or employee shall be so notified and may then make the proposed investment in full reliance upon the findings of the Chairman of the Board and Chief Executive Officer of Enron Corp.

In the event the Chairman of the Board and Chief Executive Officer of Enron Corp. should desire to make such an investment, he may do so only upon approval of the majority of a quorum of the Executive Committee of the Board of Directors of Enron Corp., other than himself, at any regular or special meeting of such Committee.

Every officer and employee shall be under a continuing duty to report, in the manner set forth above, any situation where by reason of economic or other interest in an enterprise there is then present the possibility of a conflict or disparity of interest between the officer or employee and the Company. This obligation includes but is not limited to (1) any existing

personal investment at the date of promulgation of this policy, (2) any existing personal investment at the time of employment of any officer or employee by the Company, and (3) any existing personal investment, whether or not previously approved, which may become in conflict with the provisions of this policy because of changes in the business of the Company or changes in the business of the outside enterprise in which investment has been made.

In the event of a finding by the Chairman of the Board and Chief Executive Officer of Enron Corp. (or by the Executive Committee of the Board of Directors of Enron Corp., if applicable) that a material conflict or disparity of interest does exist with respect to any existing personal investment of an officer or employee, then, upon being so notified, the officer or employee involved shall immediately divest himself or herself of such interest and shall notify the Chairman and Chief Executive Officer of Enron Corp. (or the Executive Committee, if applicable) in writing that he or she has done so.

Responsibility for Reporting

The Company has established a reporting system that allows officers, employees, and other agents of the Company to report violations of any of the Policies set forth in this booklet, or other Company policies, as well as any suspected criminal conduct by any officer, employee, or agent of the Company relating to the performance of his or her duties.

Upon observing or learning of any such violation or criminal conduct, employees should report the same by writing a letter describing the suspected violation or criminal conduct with as much detail as possible and sending the letter to:

Enron Compliance Officer
CONFIDENTIAL - Conduct of Business Affairs
P. O. Box 1188
Houston, Texas 77251-1188.

Employees may also report the same by telephoning the Office of the Chairman of the Company at (713) 853-7294 or sending ccmail addressed to the **Office of the Chairman.** If an employee places the call from his or her extension, or an outside line, the message will be completely anonymous. Similarly, ccMail addressed to the **Office of the Chairman** will also be completely anonymous.

The employee may (but is not required to) sign the letter or ccMail. Anonymous letters and anonymous ccMail will be investigated and acted upon in the same manner as letters and ccMail which contain a signature. All letters and ccMail should contain as much specific detail as possible to allow the Company to conduct an investigation of the reported matter.

All letters , ccMail, and telephone calls submitted shall be kept in confidence and acted upon only by designated objective Company personnel unless disclosure is required or deemed advisable in connection with any governmental investigation or report, in the interest of the Company, or in the Company's legal handling of the matter. The Company will not condone any form of retribution upon

any employee who uses the reporting system in good faith to report suspected wrongdoers, unless the individual reporting is one of the violators. The Company will not tolerate any harassment or intimidation of any employee using the reporting system.

EC 38015918.1

It is a condition of employment that each employee accept the responsibility of complying with the foregoing policies. The Company will require each employee of the Company to complete and submit a statement in a form designated by the Company pertaining to such employee's compliance with the policies set forth in this booklet. The Company reserves the right to request any employee to complete and submit such statement at any time or as frequently as the Company may deem advisable.

The Chairman of the Board and Chief Executive Officer of Enron Corp. may from time to time at the Chairman's discretion delegate any of the responsibilities to be fulfilled by the Chairman as hereinabove set forth. Such delegation may be made to any executive officer of the Company.

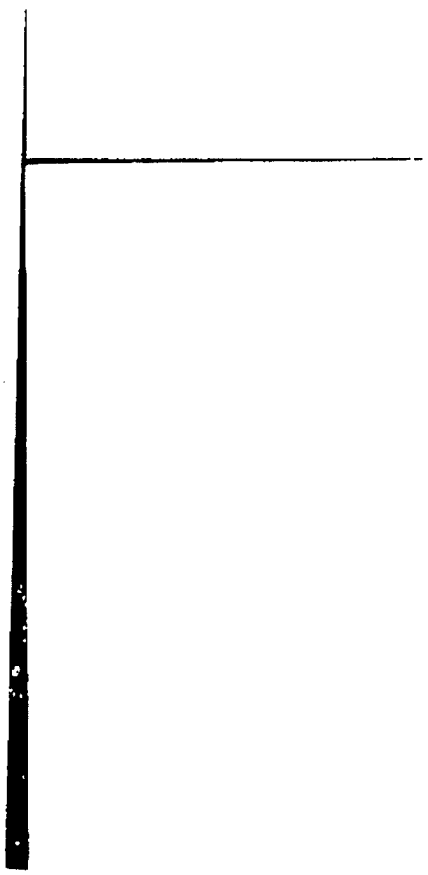
An employee who violates any of these policies is subject to disciplinary action including but not limited to suspension or termination of employment, and such other action, including legal action, as the Company believes to be appropriate under the circumstances.

EC 38015919.1

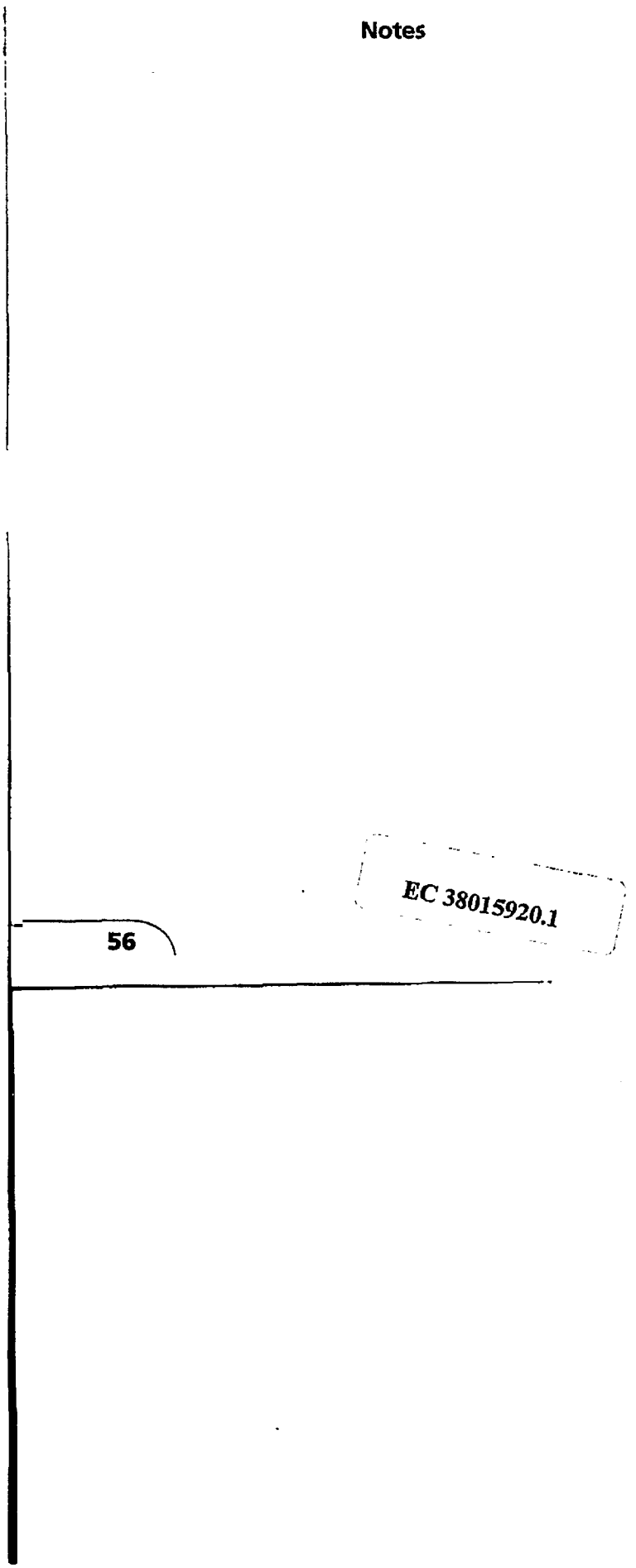
Notes

EC 38015920

55



Notes



EC 38015921